PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 11/00

A2

(11) International Publication Number: **WO 99/59375**

(43) International Publication Date: 18 November 1999 (18.11.99)

(21) International Application Number: PCT/EP99/03085

(22) International Filing Date: 5 May 1999 (05.05.99)

(30) Priority Data:
981028 8 May 1998 (08.05.98) FI

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventors: AUVINEN, Jussi, Antero; Munterinkatu 12 A 6, FIN–20360 Turku (FI). TOIVONEN, Marko, Johannes; Pormestarinkatu 8 I 75, FIN–20750 Turku (FI).

(74) Agent: BORENIUS & CO. OY AB; Kansakoulukuja 3, FIN–00100 Helsinki (FI).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SERVICE PROVIDER ACCESS METHOD AND APPARATUS

(57) Abstract

A method of providing access for a subscriber terminal (8) to services of an Internet Service Provider (ISP, 6) through the Internet (1). The terminal (8) is connected to the Internet (1) via an Internet Access Server (IAS, 8) and transmits a log–on request to a node (9) in the Internet (1). The node (9) comprises a database (11) containing authentication data relating to subscribers of a home network which controls the node (9). The terminal (8) is authenticated using the database (11) and authentication data is returned to the terminal (8). Part of the authentication data is then transmitted from the terminal (8) to the ISP (6), which in turn transmits an authentication request to the authentication node (9). The node (9) returns an authorisation to the ISP (6) and, in response, the ISP (6) allows the subscriber terminal (8) to access its services.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SERVICE PROVIDER ACCESS METHOD AND APPARATUS

Field of the Invention

The present invention relates to a service provider access method and apparatus and in particular, though not necessarily, to the collection of charge data for accessing an Internet service provider via the Internet.

Background to the Invention

The conventional way for a home user of a personal computer (PC) to access the Internet is to set up a telephone call, via his telephone operator provided with a modem pool, to an Internet service provider. The service provider allocates an Internet address to the PC ("subscriber terminal") for the duration of a session and acts as a router and protocol converter for data transmitted between the Internet and the subscriber terminal.

More recently, it has been proposed to combine the functionality of the Internet service provider into certain exchanges of the telephone network. An advantage of this is that the subscriber need only receive a single bill for both telephone calls and Internet access.

Exchanges provided with this facility are accessed by subscribers dialing a predefined access number. The exchanges contain intelligence (sometimes described as an "intelligent network") which enables them to recognise that a call received to this number is an Internet access request. In response, the exchange provides a connection between the subscriber terminal (or rather "line") and the Internet via one of a number

of so-called Internet Access Servers (IASs) - alternatively known as Network Access Servers (NASs). An IAS acts as a multiplexer/demultiplexer between a number of low capacity subscriber lines and a high capacity trunk line connecting to the Internet. The IAS also acts as a protocol converter, converting the circuit switched protocol of the telephone network into a packet Internet protocol and *vice versa*. In the case of digital cellular telephone networks (e.g. the Global System for Mobile Communications), an IAS may be accessed from a mobile terminal using a special signaling protocol to set up a data channel between the IAS and the mobile terminal.

It is often the case that a subscriber connects, via the Internet, to some remote Internet Service Provider (ISP) - sometimes referred to as a "content provider" - who offers chargeable services to the subscriber, or with whom orders for products may be placed. In this case, it is possible to transmit charging information from the ISP to the IAS and through that to the billing coordinator of the access network.

This solution to the problem of providing a subscriber with a single bill covering both telephone and Internet services works satisfactorily providing that the subscriber only wishes to access the Internet via his own or "home" telephone network. More and more however, subscribers are demanding service mobility - the ability to access the Internet from various geographical locations not covered by the home network but instead where Internet access is available via some other means (e.g. the telephone network of some "foreign" operator or a local area network). This is particularly true in the case of mobile cellular telephone subscribers who

may be able to roam across national borders with a single piece of communication hardware.

In order to meet this demand for mobility and for the amalgamation of charges into a single bill, it is necessary to provide firstly for the authentication of subscribers attempting to access the ISP via a visitor telephone network, and secondly for the repatriation of charging information to the subscribers' home telephone networks.

Summary of the Invention

It is an object of the invention to overcome or at least mitigate the disadvantages of known Internet charging systems *vis-à-vis* the combining of telephone and Internet charging data whilst providing for subscriber mobility.

According to a first aspect of the present invention there is provided a method of providing access for a subscriber to services of a service provider through a data network, the subscriber being a subscriber of a home interface network, the method comprising the steps of:

connecting a subscriber terminal to said data network;

transmitting a log-on request for the subscriber terminal from the terminal to a node in the data network, said node having a data network address and comprising a database containing authentication data relating to subscribers of the home interface network which controls said node;

authenticating the subscriber terminal using the data contained in said database and returning authentication data to the subscriber terminal;

transmitting at least part of the authentication data from the subscriber terminal to the service provider;

transmitting an authentication request from the service provider to the authentication node, and returning an authorisation to the service provider; and

in response to receipt of authorisation from the authentication node, allowing the subscriber terminal to access services of the service provider via the data network.

As the node comprising the authentication database is controlled by the home network, the node can be trusted to provide secure authentication data to the interrogating service provider.

Embodiments of the present invention enable the authentication of a subscriber terminal connected to the data network and hence the confirmation of the right of the service provider to charge the subscriber terminal for the right to access its services. Charging information may then be repatriated to the subscriber terminal's home network where it may be incorporated into a single charging system maintained by the home network.

Preferably, the data network is the Internet and said node is an Internet node having an Internet Protocol (IP) address, e.g. a Universal Resource Locator (URL) address. More preferably, the home network comprises a telecommunication network, such as a Public Switched Telephone Network (PSTN) having an Internet access server or a modem pool. Alternatively, the telecommunication network may be a cellular radio telephone network having a direct access gateway.

The subscriber terminal may be connected to the data network via a visitor network comprising a PSTN and an access server or modem pool, similar to the home network. Alternatively, connection to the data network may be through a local area network and an Internet access server.

The database of the authentication node may contain the home number of the subscriber (A-number), together with a Username and a password. Said log-on request then contains the Username and password which are verified by the node, together with a network address allocated to the subscriber terminal in the data network.

The authentication data returned to the subscriber terminal preferably comprises an access computer program and a user identification (UID). This computer program may be in the form of an applet which causes the subscriber terminal to transmit, at regular intervals, a confirmation message to the authentication node. At least the UID is then transmitted from the subscriber terminal to the service provider. The service provider polls the network node, using the terminal's network address and UID to confirm the continued authorisation of the terminal.

In an embodiment of the invention, the home network has control of a second node in the data network, which node also has an address in that network and acts as a collector of charging information for the service provider. More preferably, the authentication node records charging data for the subscriber terminal and subsequently transfers this to the charging node.

In an alternative embodiment of the invention, the service provider has permission to access a second authentication node controlled by said visitor network

or another "foreign" network. The method comprises the further step of transmitting an authentication request on behalf of the subscriber terminal to the second authentication node. When the "home" node has verified that the terminal is a subscriber of said home network, the second authentication node communicates with the home authentication node, to both authenticate the subscriber terminal and to receive subscriber identity data, e.g. the subscriber's telephone number (A-number). The second authentication node then transfers charging data to a charging node of the service provider. The charging node of the service provider can then forward charging information to the charging node of the home network.

Individual charging requests may be made from the charging node of the service provider to the authentication node of the home network. These requests may then be referred by the authentication node of the home network to the subscriber terminal for approval or rejection. The decision of the subscriber terminal is then transferred back to the service provider's charging node via the home network's authentication node.

According to a second aspect of the present invention there is provided apparatus for providing access for a subscriber to services of a service provider through a data network, the subscriber being a subscriber of a home interface network, the apparatus comprising:

connection means for connecting a subscriber terminal to a data network;

a data network node having a data network address and comprising a database containing authentication data relating to subscribers of the home interface network which controls said node;

first transmission means for transmitting a log-on request for the subscriber terminal from the terminal to said node;

means for authenticating the subscriber terminal using the data contained in said database and for returning authentication data to the subscriber terminal;

second transmission means for transmitting at least part of the authentication data from the subscriber terminal to the service provider;

third transmission means for transmitting an authentication request from the service provider to the authentication node, and returning an authorisation to the service provider; and

processing means arranged, in response to receipt of authorisation from the authentication node, to allow the subscriber terminal to access services of the service provider via the data network.

Brief Description of the Drawings

For a better understanding of the present invention and in order to show how the same may be carried into effect reference will now be made, by way of example, to the accompanying drawings, in which:

Figure 1 shows schematically an Internet access network;

Figure 2 is a flow diagram illustrating the method of operation of the network of Figure 1; and

Figure 3 shows schematically a first modification to the network of Figure 1.

Detailed Description of Embodiments

With reference to Figure 1, there is illustrated an Internet access network in which the Internet is

identified by the reference numeral 1. Point-to-point connections (i.e. logical connections) made via the Internet 1 are identified by dashed lines whilst physical connections are identified by solid lines. A terminal (e.g. personal computer) 2 is a subscriber of a public switched telephone network (PSTN) 3 and is connected thereto by a modem (not shown) and a subscriber line 4. This PSTN 3 is referred to hereinafter as the "home" network of the subscriber terminal 2. By calling a predefined access number (B-number) the subscriber terminal 2 is able to gain access to the Internet 1 through an Internet access server (IAS) 5 operated by the operator of the PSTN 3. The IAS 5 provides appropriate protocol conversion (i.e. between circuit-switched and packet-switched data transmission) for data transfer between the Internet 1 and the subscriber terminal 2.

As Internet communications for the subscriber terminal 2 are handled by the home network's own IAS 5, the home network is able to combine charges made for the Internet access, with normal telephone charges. The operator is therefore able to issue the subscriber with a single bill covering both services. Furthermore, if the subscriber terminal 2 accesses a remote Internet Service Provider (ISP) 6 which levies a charge for the service provided, charging information may be returned to the home network 3 for incorporation into this same bill.

Consider now the situation where the subscriber connects to the Internet via an IAS 7 of a local area network (LAN - not shown in Figure 1) and not through his home network. This situation is illustrated in Figure 1 where the subscriber terminal is indicated by the reference numeral 8. Before the subscriber terminal can gain access to the ISP 6, an authentication and

authorisation procedure must be completed. This makes use of a first Internet node 9, termed a Datanet User Service DataBase (DUSDB), and a second Internet node 10, termed an Internet Billing Coordinator (IBC). Both of these nodes 9,10 have assigned thereto respective IP addresses such that they represent end-points for data packets tunneled via the Internet. The IP address of the DUSDB 9 is in the form of a Universal Resource Locator (URL) address.

The DUSDB 9 is provided with a database 11 containing the following tables (further explanation of the table fields is given below):-

1. Subscriber telephone numbers in the home network (A-number), a username, and a user password. This information is used for subscriber authentication.

2. Connection start time, connection disconnect time, disconnect method, username, random part of UID, originating IP address. This table is used to store log data from subscriber login and logout sessions.

3. Connection start time, username, UID, originating IP address, latest verification time. This table is used to enhance system performance. It is used to store information after login and before logout. Upon logout, the information is transferred to table 2 and missing fields are inserted there. The latest verification time is the time that the most recent verification was received from the user applet.

4. ISP IP address, request time, UID. This table contains information on every query made by an ISP to the DUSDB.

The DUSDB 9 and the IBC 10 are both under the control of the home network 3 and can therefore be considered as secure.

In the procedure to be described below, communications between the ISP 6, the DUSDB 9, and the IBC 10, require that the identity of the transmitting and receiving identity be confirmed. This is achieved using an authentication protocol such as Radius. Communications made using this protocol are indicated in Figure 1 by the symbol Δ. Other communications over the Internet can
be made using the https protocol, indicated in Figure 1 by the symbol Φ.

The first stage in granting the subscriber terminal 8 access to the ISP 6, involves the subscriber terminal 8 logging on to the DUSDB 9. This requires the subscriber terminal to request from the IAS 7 an Internet protocol (IP) address. Logging on is achieved in a similar manner to that used for gaining Internet access to bank services. The user first enters the URL of the DUSDB 9 and then sends to the DUSDB 9 the terminal's username and (changing) password. When the DUSDB 9 has confirmed the identity of the subscriber, the DUSDB 9 sends an applet to the subscriber terminal 8, together with a user identification (UID). The applet is installed in the subscriber terminal 8 and causes the terminal to send a confirmation message to the DUSDB 9 at regular intervals, e.g. every one minute. If this message is not received by the DUSDB 9 within a certain time frame, the user is logged off from the DUSDB 9. For a general introduction to applets, see for example "Java in a Nutshell", David Flanagan, 2nd Ed, Chapter 6 (ISBN 1-56592-262-X).

When the subscriber terminal 8 has successfully logged on to the DUSDB 9, the terminal makes an https connection to the ISP 6. The ISP 6 then contacts the DUSDB 9, using the terminal's IP address and UID, to confirm whether or not the subscriber terminal 8 is logged on to the DUSDB 9. A confirmation message is returned to the ISP 6 by the DUSDB 9, and the ISP grants access to the terminal 8.

In the event that the applet generated message is not sent to the DUSDB 9 within the required time frame, the DUSDB logs off the subscriber terminal 8, and sends a message to this effect to the ISP 6 which terminates the subscriber terminal's access.

The operation of the network of Figure 1 is illustrated by the flow chart of Figure 2.

The solution to providing a single bill for telephone and ISP access of Figure 1 works satisfactorily providing that the ISP 6 has an appropriate agreement with the subscriber's home network 3. If this is not the case, then means must be provided for enabling the operator of the ISP 6 to collect charging information, including subscriber identity information, so that the operator can bill the home network 3 for services used. The home network 3 may then pass on the charges to the subscriber using its own charging system.

A network for achieving this solution is illustrated schematically in Figure 3, where elements already discussed with reference to Figure 1 are identified with like reference numerals (the subscriber's home network is omitted in the interest of simplicity). The network makes use of communication between the DUSDB 9 controlled by the home network and a second DUSDB 12.

The second DUSDB 12 is under the control of a foreign network, with the ISP 6 having a suitable agreement with that network such that the ISP 6 has permission to connect to and use the services of the DUSDB 12.

As described with reference to Figures 1 and 2, the subscriber 8 starts by logging on to the DUSDB 9 of the home network using his Username and password, and receives therefrom an applet and UID. When the subscriber 8 subsequently requests access to the ISP 6, the ISP 6 communicates with its own trusted DUSDB 12 and recognises that the subscriber 8 does not have an account with the ISP 6 and moreover that the ISP 6 does not have an appropriate service agreement with the home network 3. The ISP DUSDB 12 then contacts the home DUSDB 9 and receives thereform all data necessary for billing the subscriber 8, including the subscriber's home telephone number (A-number).

The foreign network has its own IBC node 13, which receives the necessary billing information from the network's DUSDB 12. When the subscriber's connection is terminated, the IBC 13 sends an Internet Charging Data Record (CDR) to the foreign network's billing system (not shown) which in turn forwards a note of the charges to the home network's billing system.

It will be appreciated by the person of skill in the art that modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, the network may include means for providing the subscriber with the opportunity to accept or reject individual charging requests made by the ISP 6. For each CDR generated by the IBC 13 in response to one or more charging information packets received by it from the ISP 6, the IBC 13 requests authorisation from the home network's DUSDB 9. The

DUSDB 9 directs this request to the subscriber terminal 8 using the previously transferred applet. If the subscriber accepts the request, then an OK message is sent via the DUSDB 9 and the IBC 13 to the ISP 6.

Claims

1. A method of providing access for a subscriber to services of a service provider through a data network, the subscriber being a subscriber of a home interface network, the method comprising the steps of:

connecting a subscriber terminal to said data network;

transmitting a log-on request for the subscriber terminal from the terminal to a node in the data network, said node having a data network address and comprising a database containing authentication data relating to subscribers of the home interface network which controls said node;

authenticating the subscriber terminal using the data contained in said database and returning authentication data to the subscriber terminal;

transmitting at least part of the authentication data from the subscriber terminal to the service provider;

transmitting an authentication request from the service provider to the authentication node, and returning an authorisation to the service provider; and

in response to receipt of authorisation from the authentication node, allowing the subscriber terminal to access services of the service provider via the data network.

2. A method according to claim 1, wherein the data network is the Internet and said node is an Internet node having a Universal Resource Locator (URL) address.

3. A method according to claim 2, wherein the home network comprises a telecommunication network, such as a Public Switched Telephone Network (PSTN) having an Internet access server or a modem pool.

4. A method according to any one of the preceding claims and comprising connecting the subscriber terminal to the data network via a visitor network comprising a PSTN and an access server or modem pool.

5. A method according to any one of claims 1 to 3 and comprising connecting the subscriber terminal to the data network via a local area network and an Internet access server.

6. A method according to any one of the preceding claims, wherein said database of the authentication node contains the address of the subscriber in the home network, together with a Username and a password, and said log-on request contains the Username and password which are verified by the node, together with a network address allocated to the subscriber terminal in the data network.

7. A method according to any one of the preceding claims, wherein the authentication data returned to the subscriber terminal comprises an access computer program and a user identification (UID), and at least the UID is then transmitted from the subscriber terminal to the service provider.

8. A method according to claim 7, wherein the service provider polls the network node, using the terminal's network address and UID to confirm the continued authorisation of the terminal.

9. A method according to any one of the preceding claims, wherein the home network has control of a second node in the data network, which node also has an address in that network and acts as a collector of charging information for the service provider.

10. A method according to claim 9 and comprising recording at the authentication node charging data for the subscriber terminal, and subsequently transferring this data to the charging node.

11. A method according to any one of claims 1 to 8, wherein the service provider has permission to use the services of a second authentication node controlled by a foreign network, and the method comprises the steps of:

transmitting an authentication request on behalf of the subscriber terminal to the second authentication node;

when the second node has verified that the terminal is a subscriber of said home network, communicating between the second authentication node and the authentication node of the home network, to both authenticate the subscriber terminal and to receive subscriber identity data;

transferring charging data to a charging node accessible to the service provider from the second authentication node; and

forward charging information to the charging node of the home network from the charging node of the service provider.

12. A method according to claim 11 and comprising:

forwarding individual charging requests from the charging node of the service provider to the authentication node of the home network;

referring these requests to the subscriber terminal for approval or rejection; and

transmitting the decision of the subscriber terminal back to the service provider's charging node via the home network's authentication node.

13. Apparatus for providing access for a subscriber to services of a service provider through a data network,

the subscriber being a subscriber of a home interface network, the apparatus comprising:

connection means for connecting a subscriber terminal to a data network;

a data network node having a data network address and comprising a database containing authentication data relating to subscribers of the home interface network which controls said node;

first transmission means for transmitting a log-on request for the subscriber terminal from the terminal to said node;

means for authenticating the subscriber terminal using the data contained in said database and for returning authentication data to the subscriber terminal;

second transmission means for transmitting at least part of the authentication data from the subscriber terminal to the service provider;

third transmission means for transmitting an authentication request from the service provider to the authentication node, and returning an authorisation to the service provider; and

processing means arranged, in response to receipt of authorisation from the authentication node, to allow the subscriber terminal to access services of the service provider via the data network.

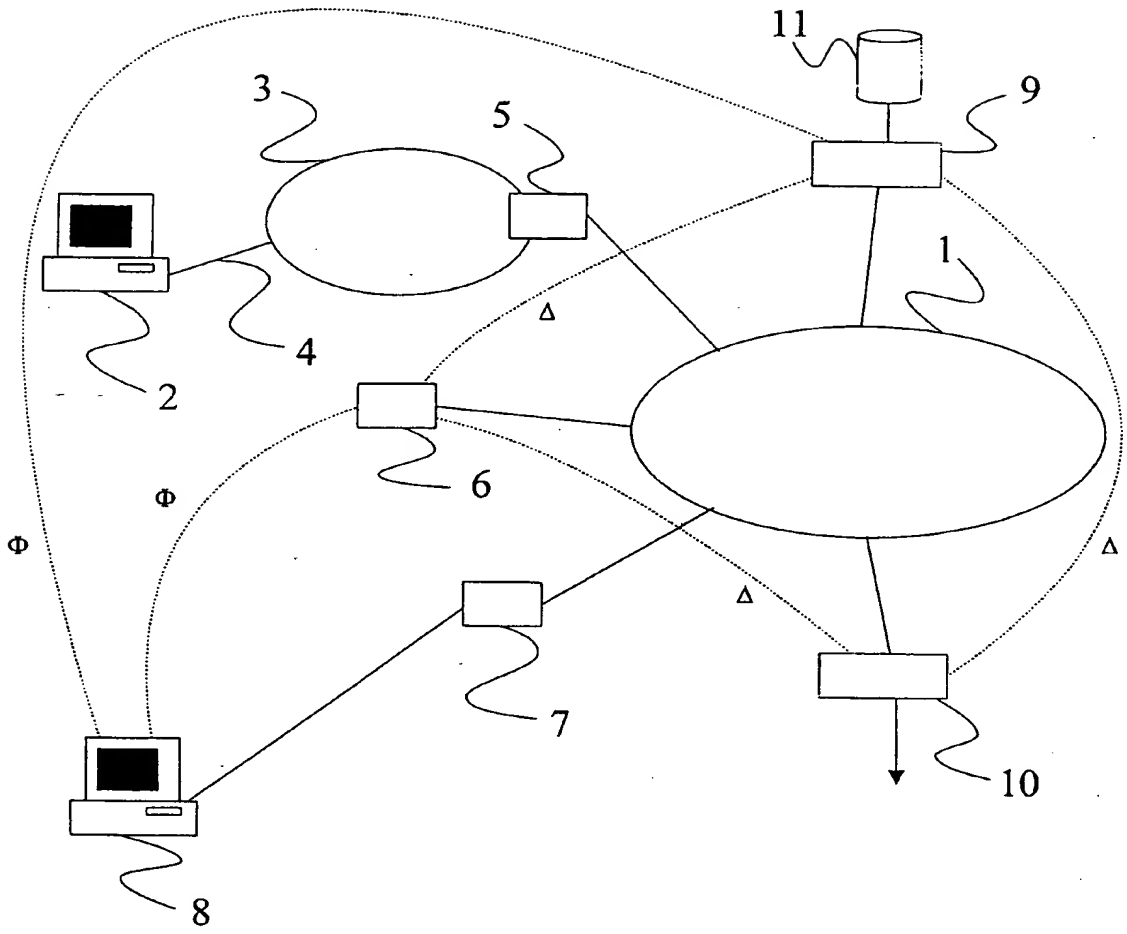

Fig. 1

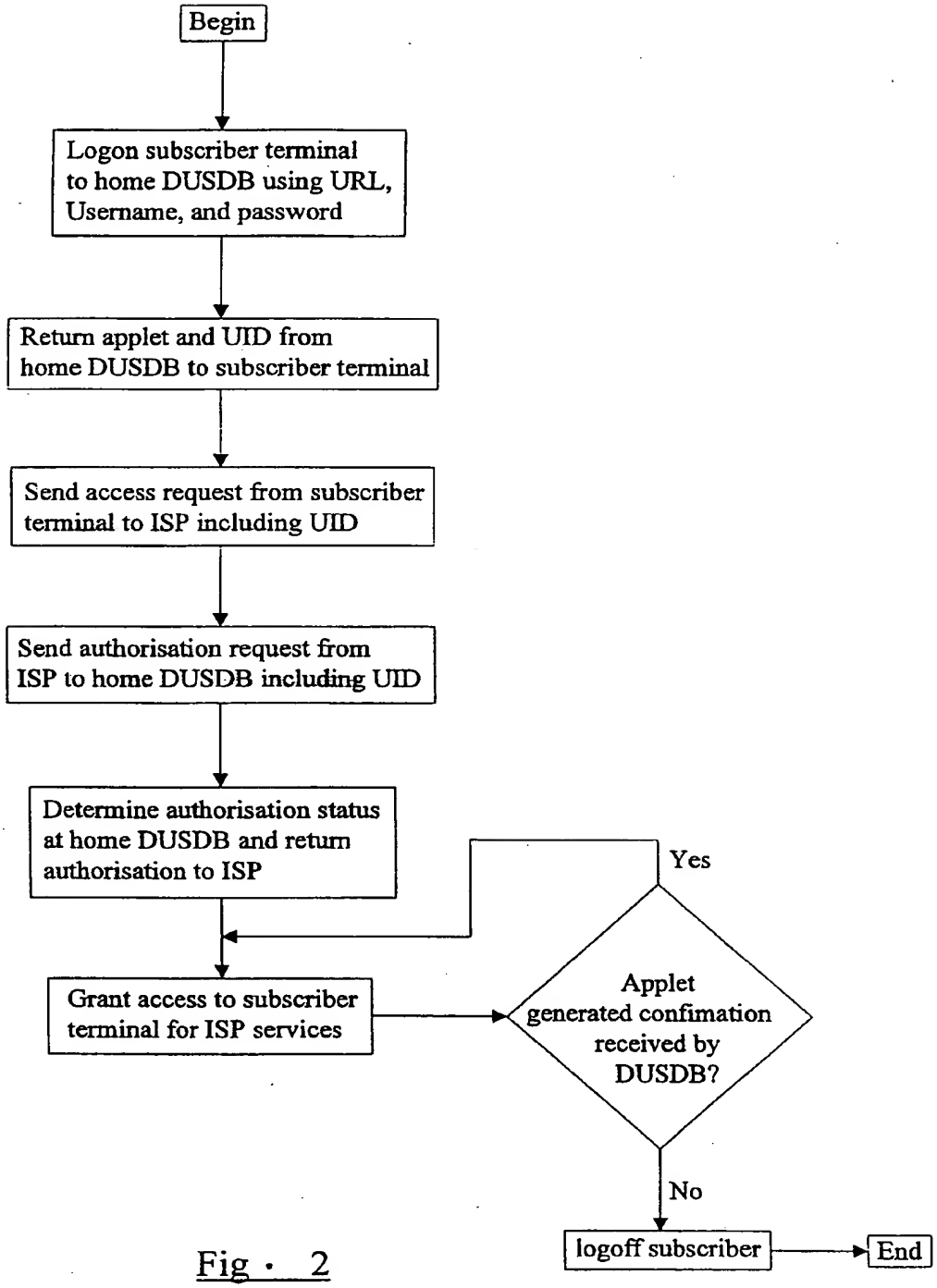
Begin
Logon subscriber terminal to home DUSDB using URL, Username, and password
Return applet and UID from home DUSDB to subscriber terminal
Send access request from subscriber terminal to ISP including UID
Send authorisation request from ISP to home DUSDB including UID
Determine authorisation status at home DUSDB and return authorisation to ISP
Grant access to subscriber terminal for ISP services
Applet generated confimation received by DUSDB?
Yes
No
logoff subscriber
End

Fig. 2

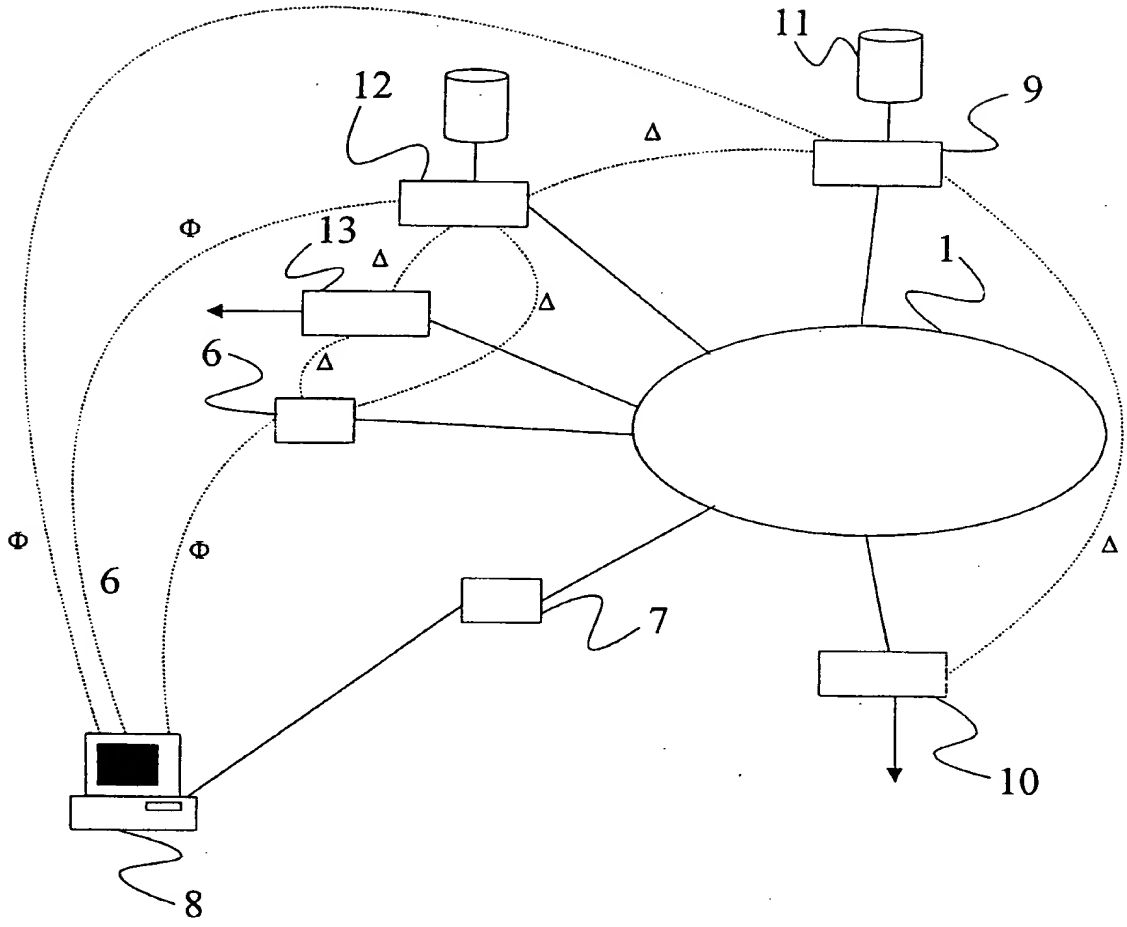

Fig. 3